A.D.B.S.

21 et 22 octobre 2002

Fiabilité de l'information et fragilité de l'Internet

Pierre BARTHELEMY
Institut de Mathématiques de Luminy
IML - UPR 9016 CNRS
Campus de Luminy - Case 907
13288 MARSEILLE Cedex 9
Tél 04-91-26-96-71 / Fax 04-91-26-96-55
barthelemy@iml.univ-mrs.fr

Conventions typographiques

⇨ Introduit une définition ou un concept clé.

o Introduit la définition d'un acronyme.

➡ introduit un item d'une énumération.

↗ introduit un URL.

Copyright

⇨ La reproduction partielle est autorisée sauf à des fins commerciales et sous réserve de la mention d'origine.

Information et désinformation

⇨ L'Internet, qui est historiquement un réseau pour la recherche ("academic network") est un outil :

- de diffusion de l'information ;
- d'accès à l'information ;
- de veille technologique.

⇨ Mais son évolution au cours des années 90 vers la "Net economy" (ou "nouvelle économie") a fait qu'il est aussi devenu un outil :

- de désinformation ;
- de guerre économique.

Actions malveillantes

➪ Les actes de malveillance existent depuis longtemps sur l'Internet (par exemple le ver Internet du 2 novembre 1988).

➪ Mais leur nombre a fortement augmenté depuis quelques années.

➪ A l'heure où l'Internet devient un vecteur de l'économie mondiale (développement du commerce électronique et plus généralement de la "Net economy"), toute capacité de nuisance devient une arme dans la guerre économique.

➪ De nouvelles formes de délinquance se développent.

Les formes de la menace

⇨ En matière de sécurité des systèmes d'information, les menaces sont diverses et les motivations peuvent être classées en quatre catégories :

- menace ludique ;
- menace cupide ;
- menace terroriste (organisations) ;
- menace stratégique (gouvernements) ;
- l'interpénétration : imbrication dynamique des menaces précédentes.

⇨ La menace appelle une réaction sociale : connaissance, prévention, répression.

⇨ Il y a risque lorsqu'il y a conjonction d'une menace et d'une vulnérabilité.

menace x vulnérabilité = risque

Un sujet d'actualité

⇨ La sécurité des systèmes d'information est un sujet d'actualité :

- commerce électronique ;
- vulnérabilité des infrastructures ;
- interceptions des communications ;
- intelligence économique ;
- protection de la vie privée et des données personnelles.

Des activités diverses

⇨ Les activités délictueuses dépassent le cadre de l'Internet :

➡ phreaking ;
piratage de PABX, fraude téléphonique

➡ carding ;
fraude à la carte bancaire

➡ war-driving ;
piratage de réseaux sans fil (une promenade en voiture dans Paris en avril 2002 a permis de détecter 80 réseaux en 3 heures). Cartographie sur le Web.

➡ hacking.
piratage informatique

Les causes de l'insécurité

➡ la concentration des informations sur des serveurs connectés à l'Internet ;

➡ l'interconnexion des réseaux et leur ouverture vers l'Internet :

➡ les logiciels propriétaires (hégémonie et manque d'informations) ;

➡ la technologie et l'information technique accessibles à tous ;

➡ la nature humaine (faiblesses, vénalité) ;

➡ le manque de formation, une culture sécurité insuffisante ;

➡ la conception d'Internet (réseau ouvert, protocoles non sécurisés).

Un niveau de protection insuffisant

➪ Les entreprises ne se protégent pas suffisament pour diverses raisons :

- manque de budget (50%) ;
- manque de personnel (40%) ;
- manque de temps (20) ;
- réticence du management (15%) ;
- méconnaissance des enjeux (15%) ;

Source : Forrester Research, oct.2000

La sécurité d'un système d'information

⇨ On appelle sécurité d'un système d'information l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures prises pour assurer:

➡ la **confidentialité**, c'est-à-dire le caractère réservé d'une information dont l'accès est limité aux personnes admises à la connaître pour les besoins du service;

➡ la **disponibilité**, qui est l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances ;

➡ l'**intégrité** du système et de l'information, qui garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime.

➡ lorsque l'information est échangée, l'intégrité s'étend à l'**authentification** du message, c'est-à-dire à la garantie de son origine et de sa destination.

Source : recommandation n°901/DISSI/SCSSI.

Confidentialité

➪ Le but est de garder des informations secrètes.

Seuls des utilisateurs autorisés doivent y avoir accès.

Intégrité

➪ Le but est de préserver des informations contre les modifications.

Seuls des utilisateurs autorisés doivent pouvoir modifier ces informations.

Authentification

⇨ Le but est de garantir l'identité d'un utilisateur pour contrôler les droits d'accès afin de rendre un service de sécurité.

Disponibilité

⇨ Le but est de garantir la possibilité d'accèder aux informations.

Attaques contre des serveurs WWW

⇨ Les attaques contre des serveurs WWW ont pour but de leur faire servir de fausses pages HTML en modifiant des pages existantes ou en créant de nouvelles pages.

Exemples : FBI, Altavista, Air Tran, US Air Force.

⇨ Ces attaques utilisent des failles de sécurité dans les daemons HTTP.

⇨ Rappel : un serveur WWW est une machine qui fait tourner un daemon HTTP.

- daemon : deferred auxilliary execution monitor
- HTTP : HyperText Transfert Protocol.

Fonction en cause : intégrité.

➪ Préjudices pour les sites victimes de ce type d'attaque : image de marque, notoriété, perte de clientèle.

➪ Les attaques de ce type sont très fréquentes (2000 sites en France pendant l'été 2000).

Les nombreuses failles de I.I.S.

➪ Les attaques contre des serveurs WWW sont fréquentes contre les serveurs I.I.S. de Microsoft.

➪ En mai 2001, un patch général de sécurité pour I.I.S. a été diffusé.

Il rassemble les 22 patches pour I.I.S. 4.0 sortis depuis le service pack 5 de Windows NT 4.0 et les 16 patches pour I.I.S. 5.0.

Web spoofing

⇨ principe : le pirate construit un faux serveur WWW auquel s'adresse la victime en croyant s'adresser au vrai serveur.

⇨ menace : le pirate contrôle tout ce que fait la victime : saisie de mots de passe, de numéros de carte de crédit, ...

⇨ une attaque par Web spoofing se déroule de la manière suivante :

➡ amener la victime à entrer dans le faux serveur (i.e. à se connecter au faux serveur) ;

➡ intercepter les requêtes destinées au vrai serveur ;

➡ récupérer les vraies pages ;

➡ modifier les vraies pages ;

➡ envoyer les fausses pages à la victime.

⇨ JavaScript permet d'améliorer l'attaque en permettant au pirate de :

➡ ré-écrire la ligne de localisation ;
➡ ré-écrire la ligne d'événements ;
➡ changer des actions des menus.

⇨ les seules parades sont de :

➡ désactiver JavaScript ;
➡ s'assurer que la ligne de localisation est visible ;
➡ être très attentif et méfiant.

Fonctions en cause : authentification, intégrité.

⇨ Les attaques de ce type sont peu fréquentes, car difficiles à réaliser.

Attaques contre le DNS

➪ La résolution des noms est assurée par des machines dites serveurs de noms ("nameservers"), ou serveurs DNS.

o D N S : Domain Name System.

➪ Des failles de sécurité sont régulièrement découvertes dans le logiciel Bind, aujourd'hui développé par l'ISC, et utilisé par les serveurs DNS.

➪ Ces attaques sont anciennes (exemple : AlterNic) mais restent fréquentes, voire quotidiennes en 2000.

➪ De nouvelles failles majeures, découvertes en décembre 2000, ont été signalées en janvier 2001 par le CERT de l'Université Carnegie Mellon.

➪ Une vulnérabilité de Bind 9 vis-à-vis d'attaques en déni de service a été signalée en juin 2002

Les cookies WWW

⇨ Les cookies sont des requêtes émises par un serveur WWW en direction d'un client WWW (navigateur) afin de se faire communiquer des informations sur la configuration ou l'identification du client.

⇨ Les cookies sont généralement utilisés par des serveurs commerciaux pour construire un profil de l'utilisateur.

⇨ L'offre de mise à disposition de services en ligne personnalisés masque souvent une stratégie de recueil d'informations personnelles à des fins purement commerciales.

⇨ L'objectif est de connaître les identités, centres d'intérêts, habitudes, préférences des utilisateurs, en vue d'actions de marketing ciblées.

Fonction en cause : confidentialité.

Un conseil de configuration

⇨ Il est toujours possible (et recommandé) de désactiver (refuser) les cookies dans la configuration du navigateur.

⇨ D'une manière générale, il est recommandé de se méfier de JavaScript, de Java, d'ActiveX et des cookies.

⇨ ActiveX permet l'exécution automatique des scripts Visual Basic en pièce jointe d'un message (cf. le virus "I Love You" en mai 2000).

Les attaques du type "denial of service"

⇨ Il existe tout un ensemble d'attaques du type DoS.

o D o S : "Denial of Service".

Toutes visent à saturer ou à planter une machine cible qui ne sera donc plus en mesure de rendre les services attendus par ses utilisateurs légitimes.

➡ "ping of death" (basé sur un débordement de buffer lors de la réception d'un datagramme IP)
Apparu en 1998, il permettait alors de planter 80% des machines ;

➡ "smurfing" (basé sur des échos ICMP saturants) ;

➡ toute autre attaque saturante ("mail bombing" par exemple).

Fonction en cause : disponibilité.

Les attaques du type "distributed denial of service"

⇨ En décembre 1999, sont apparus des outils permettant des attaques d'un type nouveau, dit DDoS pour "distributed denial of service".

⇨ Les outils connus pour réaliser ce type d'attaques sont :

- trinOO ;
- TFN (Tribe Flood Network) ;
- TFN2K ;
- Stacheldraht.

➚ http://staff.washington.edu/dittrich/misc

⇨ En février 2000, ces outils ont été utilisés pour réaliser des attaques visant des sites phares de la "nouvelle économie".

⇨ Ces attaques ont été aussitôt fortement médiatisées.

Le principe des attaques du type "distributed denial of service"

⇨ Dans un premier temps, le pirate prend le contrôle d'un certain nombre de machines à travers l'Internet afin d'y installer un programme client (souvent appelé "zombie").

⇨ Le pirate utilise ensuite un programme maître qui contrôle tous les zombies et lance une attaque convergente vers un même serveur cible.

⇨ L'objectif est de saturer le serveur cible en l'inondant de paquets (attaque par "flooding").

Fonction en cause : disponibilité.

⇨ Il existe des logiciels de détection de client DDoS.

⇨ Ces attaques peuvent être contrées au niveau des routeurs et des "firewalls".

La vague d'attaques "DDoS"de février 2000

⇨ Le 7 février 2000, une attaque de type DDoS a touché Yahoo. Le site est resté hors service pendant près de trois heures.

⇨ Les 8 et 9 février 2000, des attaques similaires ont touché plusieurs autres sites : eBay, Buy.com, Amazon.com, CNN, ZDNet, E*Trade, Datek Online.

⇨ Ces attaques massives ont mis en évidence la vulnérabilité de l'Internet.

⇨ Les motivations de leurs auteurs ne sont pas connues : vandalisme ?, racket ?, intoxication ?, ...

⇨ Les cours de Yahoo!, Amazon et eBay ont chuté le 9 février 2000 à Wall Street.

Est-ce le début d'une guerre économique ?

➢ Le 9 février 2000, les attaques de type DDoS ont fait l'objet d'un bulletin d'alerte de la part d'ISS (un précédent avis avait été diffusé le 7 décembre 1999).

o I S S : Internet Security Systems.

➢ D'autres attaques se seraient produites en France (non confirmé).

➢ Le 15 février 2000, le président des Etats-Unis a réuni à la Maison Blanche une trentaine de spécialistes de la sécurité informatique pour discuter des moyens de lutter contre ces attaques.

➢ Le 18 février 2000, le site du FBI a été attaqué de la même manière et il est resté hors service plusieurs heures.

➢ Le 20 avril 2000, la police canadienne arrête à Montréal un adolescent connu sous le pseudonyme de "Mafiaboy" et soupçonné d'être l'auteur de ces attaques.

En septembre 2001, il a été condamné à huit mois de prison.

Un nouvel outil "DDoS"

➪ A la fin du mois d'avril 2000 est apparu "mstream", un nouvel outil permettant des attaques de type DDos.

➪ Il a été découvert sur le réseau de l'Université de Washington, puis signalé sur les réseaux des universités de l'Indiana et de Pennsylvanie.

➪ Le 1er mai 2000, "mstream" a fait l'objet d'un bulletin d'alerte de la part d'ISS.

➪ Jusqu'à présent, il ne semble pas avoir été utilisé pour de véritables attaques.

De nouvelles attaques "DDoS"

⇨ En janvier 2001, les principaux sites de Microsoft ont été victimes d'attaques de type DDoS.

⇨ En mai 2002, un réseau régional du réseau RENATER a été victime d'une attaque par déni de service entraînant la saturation de ce réseau régional et d'une liaison internationale.

Les serveurs FTP Warez

➪ Des logiciels, films (format DivX ou MPEG 4) et musiques (format MP3) protégés par un copyright sont librement distribués par des serveurs FTP installés à l'insu des utilisateurs et administrateurs de machines piratées.

➪ Profitant d'une faille de sécurité, le pirate installe un serveur de fichiers FTP sur une machine dont il utilise l'espace disque et la bande passante.

La messagerie électronique

➪ La messagerie électronique ne présente en général aucune garantie d'aucune sorte :

➡ pas de garantie d'authentification (l'identité réelle de l'émetteur d'un message n'est pas garantie, sauf à utiliser des techniques de signature électronique). De cette lacune découlent : spam, fake mail, rumeurs.

➡ peu de garantie de confidentialité, du moins côté client.

➡ pas de garantie de disponibilité. De cette lacune découle le mail bombing.

Le "spam"

⇨ Le "spam" est la diffusion massive de messages électroniques non désirés par leurs destinataires et généralement à caractère publicitaire.

Il est donc l'analogue du publipostage ("mailing" publicitaire).

⇨ L'adresse du véritable expéditeur est souvent masquée par l'utilisation d'un serveur tiers comme relais de messagerie.

⇨ Il est difficile de s'en prémunir (sauf à mettre en place au niveau de votre serveur de messagerie des techniques préventives comme les listes noires ou le filtrage par mots clés).

Le "mail bombing"

➪ Le "mail bombing" (littéralement "bombardement de messages") consiste à envoyer un grand nombre de messages vers un serveur de messagerie afin de le saturer (par surcharge du système ou débordement de l'espace disque).

➪ C'est une attaque du type "déni de service" ("denial of service") car le serveur visé n'est alors plus en mesure de rendre le service attendu par ses utilisateurs légitimes.

➪ Certains canulars s'apparentent à des opérations de "mail bombing".

Exemple : American Cancer Society

NB : le fait d'envoyer des messages volumineux, surtout à un grand nombre de destinataires, peut vous amener à saturer involontairement un serveur de messagerie.

Brefs rappels techniques sur les logiciels de messagerie

➪ Côté client, l'utilisateur doit disposer d'un logiciel dit MUA.

o M U A : Mail User Agent.

Exemples sur Mac : Eudora, POPMail, Pegasus Mail, techmail, leemail, Claris Emailer, Netscape Navigator, Microsoft Internet Explorer, Microsoft Outlook Express, Entourage, PowerMail.

Exemples sur PC : Eudora, Netscape Navigator, Microsoft Internet Explorer, Microsoft Outlook Express.

Exemples sous Unix : mail, xmail, mailtool, pine, elm, zmail.

➪ Côté serveur, l'administrateur doit mettre en place un logiciel dit MTA.

o M T A : Mail Transfert Agent.

Exemple : sendmail, Postfix.

Les attaques contre la messagerie électronique

⇨ Les attaques contre la messagerie électronique sont fréquentes et réalisables à plusieurs niveaux :

➡ au niveau des serveurs (MTA) :
attaques par débordement de buffer ;

➡ au niveau des clients (MUA) :
réception de fichiers exécutables en pièces jointes ;

➡ au niveau des MUA avec MIME :
des failles sur les MUA utilisant le format MIME permettent le lancement automatique d'un exécutable en pièce jointe (technique de débordement de buffer sur le nom de fichier).

o M I M E : Multi-purpose Internet Mail Extension.

Les virus propagés par la messagerie électronique

⇨ Par le biais des pièces jointes, la messagerie électronique est susceptible de propager des virus.

⇨ Il peut s'agir :

➡ de faux virus (simples rumeurs) ;

➡ de macro-virus (macros Word ou Excel). Ce cas est très fréquent (80%) ;

➡ de virus exécutables (exemple : Chernobyl en avril 1999) ;

➡ de virus exécutables à réplication (exemples : Melissa en mars 1999, Explore en juin 1999, I Love You en mai 2000).

⇨ Ils touchent surtout les utilisateurs de logiciels Microsoft (Windows, Office, Outlook, Explorer).

Le virus "I Love You"

⇨ Le virus "I Love You" (ou "LoveLetter") s'est propagé à partir du 4 mai 2000 et a causé des ravages considérables en deux jours.

⇨ Il s'agit plus précisément d'un ver (virus à réplication automatique).

⇨ Sa structure initiale était la suivante:

➡ Sujet : ILOVEYOU

➡ Corps : "kindly check the attached LOVELETTER coming from me" ;

➡ pièce jointe : un script écrit en Visual Basic (fichier LOVE-LETTER-FOR-YOU.TXT.vbs).

⇨ Il s'est répandu principalement par messagerie électronique mais seuls les utilisateurs d'Outlook Express étaient vulnérables.

⇨ Une fois lancé et installé, il envoyait des messages infectés vers toutes les adresses figurant dans le carnet d'adresses de l'utilisateur.

⇨ Techniquement, il était basé sur :

➡ ActiveX, qui permet l'exécution automatique des scripts Visual Basic en pièce jointe d'un message

➡ une faille d'Outlook Express, qui permet la re-expédition vers des adresses figurant dans le carnet d'adresses.

⇨ Il aurait touché plus de 3 millions d'ordinateurs dans le monde et causé des dommages pour un montant évalué à 8,7 milliards d'USD.

Le virus "Kournikova"

➪ Le virus "Anna Kournikova" (ou VBS/OnTheFly, ou VBS.SST@mm) s'est propagé en février 2001.

➪ Il s'agit là encore d'un ver écrit en Visual Basic (extension .vbs).

➪ Les virus ou vers de ce type sont devenus très fréquents (NakedWife est un autre exemple, apparu en mars 2001).

➪ Sa structure initiale était la suivante :

- Sujet : "Here you have, ;o)"
- Corps : "Hi : check This" ;
- pièce jointe : un script écrit en Visual Basic (fichier AnnaKournikova.jpg.vbs).

➚ http://www.cert.org/advisories/CA-2001-03.html

➪ Son auteur a été condamné aux Pays-Bas à 150 heures de travaux d'utilité publique.

Un flux permanent de virus

➪ De nouveaux virus apparaissent tous les jours. Parmi les plus connus en 2001 et 2002, on peut citer :

- Klez ;
- Sircam ;
- Magistr ;
- Hybris ;
- YaHa ;
- Nimda ;
- Frethem ;
- BadTrans.

➪ Tous ces virus sont basés sur les mêmes vulnérabilités d'Explorer, d'Outlook et d'Outlook Express.

Des précautions élémentaires

⇨ Quelques précautions élémentaires sont à respecter :

➡ installer les mises à jours des logiciels (par exemple le "Service Pack 2" et la version 6 d'Explorer) ;

➡ ne jamais cliquer sur des pièces jointes sans en connaître de manière sûre l'origine exacte ;

➡ installer et tenir à jour en permanence des anti-virus.

Cartes de visite sous Outlook

⇨ Une grave faille de sécurité, signalée en février 2001, touche presque toutes les versions d'Outlook.

⇨ Cette faille du type "buffer overflow" permet à un programmeur malveillant de faire exécuter toute action de son choix lors de l'ouverture ou du rangement d'une carte de visite virtuelle.

➚ http://www.microsoft.com/technet/security/bulletin/ms01-012.asp

⇨ Un patch a été aussitôt diffusé.

➚ http://www.microsoft.com/windows/ie/download/critical/q283908/default.asp

Quelques incidents avec la messagerie

➢ Pendant un week-end à la fin du mois d'août 1999, tous les comptes d'Hotmail ont été accessibles sans mot de passe (Hotmail est un service de messagerie gratuit proposé par Microsoft).

➢ Dans la journée du 14 janvier 2000, le serveur de messagerie électronique des abonnés de Wanadoo Câble à Bordeaux, soit environ 2300 utilisateurs, a été accessible sans mot de passe.

➢ Dans les deux cas, il semble s'agir d'incidents techniques plutôt que d'attaques (quoique ...) .

➢ Dans la deuxième quinzaine de janvier 2000, les serveurs de messagerie de Wanadoo (qui gèrent environ 1,8 millions d'adresses) ont migré vers un système qui se veut mieux sécurisé.

Actions de désinformation

⇨ Sur l'Internet se propagent par la messagerie électronique des rumeurs, légendes, fausses nouvelles, canulars, pétitions, "chaînes", mythes, ... ("hoaxes").

Exemples :

➡ annonces de faux virus (Good Times en 1994, AOL4Free en 1997, Win a Holiday en 1998) ;

➡ fausses alertes (piratage de lignes de téléphones fixes ou portables par 09#) ;

➡ "chaînes" humanitaires (Jessica) ;

➡ pétitions humanitaires (talibans) ;

➡ médisance, dénigrement, calomnie (Kentucky Fried Chicken, TotalFina) ;

➡ canulars (Nokia, Ericsson).

⇨ Le but est parfois de récupérer des adresses de messagerie électronique pour des actions de "spam" ultérieures.

⇨ Les motivations de leurs auteurs, qui vont des mauvais plaisants aux calomniateurs, sont diverses.

⇨ Mais au-delà des mauvaises plaisanteries, elles sont aussi des actions de guerre économique :

- dénigrement d'un concurrent ;
- collecte d'adresses ;
- saturation de serveurs.

⇨ En cas de doute, il est bon de consulter quelques serveurs :

- sur les rumeurs en général :
  http://www.hoaxbuster.com

- sur les nouveaux (vrais) virus
  http://www.atoutmicro.ca/viralert.htm

- sur les rumeurs et les faux virus :
  http://www.kumite.com/myths/

- sur les vrais et faux virus :
  http://www.antivirus-fr.com/infovirus/activexj.htm

La diffusion interne

⇨ Le 14 janvier 2000, des salariés d'Alsthom à Saint-Ouen étaient en grève pour protester contre un plan social découvert sur l'Intranet de l'entreprise.

⇨ Selon la direction d'Alsthom, ce document interne avait été placé par inadvertance sur l'Intranet et ne serait qu'une hypothèse de travail.

Fonction en cause : confidentialité.

⇨ Pourquoi et comment ce document s'est-il retrouvé en accès public ?

- simple bavure ?
- fuite organisée ?

⇨ La diffusion d'informations sur l'Internet doit faire l'objet d'un contrôle.

La diffusion interne

⇨ De mai à août 2000, un serveur Web à usage interne de Bull a été librement accessible sans mot de passe.

Ce serveur contenait des documents internes mais pas "hautement confidentiels" (rapports de mission, approches commerciales, produits et services vendus aux clients, ...).

Parmi les clients figuraient : Direction Générale des Impôts, Gendarmerie Nationale, EDF, Aérospatiale ...

Fuites bancaires

➪ En novembre 2000, des numéros de comptes, les adresses de leurs titulaires et des virements bancaires de vedettes du show-business pouvaient être consultés sur le site Direct Net de la banque Credit Suisse.

➪ Selon la banque, ces données avaient été mises sur son site par des tiers, étrangers à la banque.

Source : Blick (quotidien suisse), repris par le Figaro Economie du 10 novembre 2000.

Virements bancaires

⇨ En décembre 2000, des pirates ont pu détourner 34 KF suisses par virements à partir de trois comptes bancaires sur le site E-banking de l'UBS.

⇨ L'information a été confirmée par la banque. Les clients ont été dédommagés.

Source : Blick (quotidien suisse), repris par le Figaro Economie du 16 décembre 2000.

Piratage et racket

➪ Au premier trimestre 2001, plusieurs groupes de pirates d'Europe de l'Est, principalement russes et ukrainiens, ont attaqué une quarantaine de sites américains de commerce électronique situés dans une vingtaine d'états et se sont ainsi procurés plus d'un million de numéros de cartes de crédits.

➪ Les victimes étaient ensuite rackettées sous la menace de voir diffusées les informations piratées (numéros de cartes de crédits, mots de passe, données bancaires).

➪ Ces attaques étaient basées sur des vulnérabilités connues dans IIS et Windows NT depuis 1998.

➪ Malgré de précédents avis de sécurité (bulletins de sécurité Microsoft n°MS98-004, MS99-025, MS00-014, MS00-008), beaucoup d'exploitants n'avaient pas mis à jour leurs systèmes.

⇨ C'est de loin la plus vaste attaque de ce type connue à ce jour.

Sources :

* avis 2001/INFO001 du CERT-Renater "Large Criminal Hacker Attack on Windows NT E-Banking and E-Commerce Sites" du 09/03/2001 et avis 2001/VULN078 ;
* note du SANS du 08/03/01 ;
* avis du NIPC 00-060 et 01-003 ;
* Figaro Economie du 10/03/2001;

o C E R T : Computer Emergency Response Team.

o S A N S : System Administration, Networking, and Security.

o N I P C : National Infrastructure Protection Center.

La rumeur Emulex

⇨ Le 25 août 2000, le cours de la société Emulex (spécialisée dans les équipements actifs de réseau) chutait de 62% après la diffusion sur l'Internet d'un faux communiqué annonçant la démission de son président pour cause de mauvais résultats.

⇨ Bloomberg, Internet Wire, CBS Marketwatch et Dow Jones News Retrieval Service rediffusaient le faux communiqué sans l'authentifier.

⇨ Le gain pour l'auteur du faux communiqué, rapidement appréhendé, aurait été de 250.000 USD.

La perte des actionnaires d'Emulex serait de 110 millions d'USD.

⇨ Le suspect, Mark Jacob, un étudiant de 23 ans, avait travaillé chez Internet Wire jusqu'au 18 août 2000.

Pour cet acte malveillant, il avait opéré à partir d'une bibliothèque universitaire.

Un an plus tard, il était condamné à 4 ans de prison.

Nuisances diverses

➪ création de "faux" noms de serveurs, similaires aux noms de vrais serveurs.

➪ dépôt abusif de noms de domaines (on parle de "cybersquatting").

Ces conflits se jugent selon le droit des marques.

Exemples : le-monde.com, emancipez-paris.com

➪ Il peut être fait appel à l'arbitrage de l'OMPI (WIPO).

o O M P I : Organisation Mondiale de la Propriété Industrielle.

➚ http://www.wipo.org

➪ Une base de données du centre d'arbitrage et de médiation de l'OMPI répertorie les litiges.

➚ http://arbiter.wipo.int/domains/search/index-fr.html

Les "Web bugs"

⇨ Les traitements de textes (Word, StarOffice, WordPerfect, ...) permettent d'intégrer des images et maintenant d'insérer des URL.

⇨ Un URL est inséré dans un document dont l'auteur veut tracer l'usage et a pour effet, à chaque visualisation du document, de charger une image invisible (un pixel suffit) depuis un serveur.

⇨ Lors de cette connexion client-serveur (qui n'est pas perçue par l'utilisateur), le serveur récupère diverses informations concernant le client (au minimum le nom et l'adresse IP du client).

⇨ Ceci permet à l'auteur du document, par ailleurs exploitant dudit serveur, de savoir où et quand son document est ouvert.

➪ Cette technique du "Web bug" peut être combinée avec des "cookies". Un "Web bug" sous Word permet de lire et d'écrire des "cookies" d'Internet Explorer.

La protection des données

⇨ Les données véhiculées sur l'Internet sont potentiellement sujettes à des interceptions (par exemple avec des sniffers).

NB : un sniffer est un programme permettant de capturer des trames réseau.

⇨ Les données circulent à priori en clair, sauf à utiliser des techniques de cryptage.

⇨ Il est donc déconseillé de diffuser sur l'Internet des documents confidentiels.

Guerre de l'information

⇨ L'US Army a créé des unités dites de "guerre de l'information" pour intervenir sur les réseaux informatiques internationaux.

⇨ Ces unités sont notamment constituées d'officiers de réserve travaillant dans des entreprises civiles du domaine des technologies de l'information.

Source : Le Monde du 16/12/2000.

⇨ Le virus Yaha, créé par des développeurs indiens en 2002, a pour objectif de bloquer par saturation le portail gouvernemental pakistanais.

C'est l'aspect électronique du conflit opposant l'Inde le Pakistan au sujet du Cachemire.

Sources

- Internet Actu (FTpresse) :
  http://www.internetactu.com

- Le Monde :
  http://www.lemonde.fr

- Hoaxbuster :
  http://www.hoaxbuster.com

- Sécurité Informatique (CNRS) :
  http://www.cnrs.fr/Infosecu

- http://www.kitetoa.com

- http://www.clussif.asso.fr

Merci de votre attention

Les transparents du présent exposé sont disponibles en FTP anonyme à l'URL :

ftp://iml.univ-mrs.fr/
pub/barthelemy/ADBS/fiabilite.pdf

La reproduction partielle ou totale est autorisée sauf à des fins commerciales et sous réserve de la mention d'origine.

Vous pouvez me contacter par e-mail pour toutes questions : barth@iml.univ-mrs.fr

Vous êtes invités à me communiquer toute remarque quant à l'amélioration et à la tenue à jour de ce support de cours.

Pierre BARTHELEMY
Institut de Mathématiques de Luminy
IML - UPR 9016 CNRS
Campus de Luminy - Case 907
13288 MARSEILLE Cedex 9
Tél 04-91-26-96-71 / Fax 04-91-26-96-55
barthelemy@iml.univ-mrs.fr